Media Contact

Laura K. Johnson
PCI Security Standards Council
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

Payment Card Industry Security Standards Council Releases PCI Data Security Standard Version 3.2

— Data Breach Trends Drive Modifications to Global Standard for Payment Security —

WAKEFIELD, Mass., 28 April 2016 — Today the PCI Security Standards Council (PCI SSC) published a new version of its data security standard, which businesses around the world use to safeguard payment data before, during and after a purchase is made. PCI Data Security Standard (PCI DSS) version 3.2 replaces version 3.1 to address growing threats to customer payment information. Companies that accept, process or receive payments should adopt it as soon as possible to prevent, detect and respond to cyberattacks that can lead to breaches. Version 3.1 will expire on 31 October 2016.

"The payments industry recognizes PCI DSS as a mature standard, so the primary changes in version 3.2 are clarifications on requirements that help organizations confirm that critical data security controls remain in place throughout the year, and that they are effectively tested as part of the ongoing security monitoring process," said PCI Security Standards Council General Manager Stephen Orfei. "This includes new requirements for administrators and services providers, and the cardholder data environments they are responsible to protect. PCI DSS 3.2 advocates that organizations focus on people, process and policy, with technology playing an important role in reducing the overall cardholder data footprint."

The update to the standard is part of the regular process for ensuring the PCI DSS addresses current challenges and threats. This process factors in industry feedback from the PCI Council's more than 700 global Participating Organizations, as well as data breach report findings and changes in payment acceptance.

"We've seen an increase in attacks that circumvent a single point of failure, allowing criminals to access systems undetected, and to compromise card data. A significant change in PCI DSS 3.2 includes multi-factor authentication as a requirement for any personnel with administrative access into environments handling card data. Previously this requirement applied only to remote access from untrusted networks. A password alone should not be enough to verify the administrator's identity and grant access to sensitive information," said PCI Security Standards Council Chief Technology Officer Troy Leach. "Additionally, service providers, specifically those that aggregate large amounts of card data, continue to be at risk. PCI DSS 3.2 includes a number of updates to help these entities demonstrate that good security practices are active and effective."

Key changes in PCI DSS 3.2 include:

- Revised Secure Sockets Layer (SSL) and early Transport Layer Security (TLS) sunset dates as outlined in the Bulletin on Migrating from SSL and Early TLS
- Expansion of requirement 8.3 to include use of multi-factor authentication for administrators accessing the cardholder data environment
- Additional security validation steps for service providers and others, including the "Designated Entities Supplemental Validation" (DESV) criteria, which was previously a separate document.

A full copy of the new PCI Data Security Standard version 3.2, including a Summary of Changes document is available at: https://www.pcisecuritystandards.org/document_library.

PCI Perspectives blog post PCI DSS 3.2: What's New? provides more information on changes to the standard and its supporting documents. The blog also outlines additional resources available for understanding and adopting PCI DSS version 3.2.

Added Leach, "Moving forward, we expect incremental revisions like those in version 3.2 to address evolving threats to the payment landscape, with a focus on helping companies use this standard as a good framework for everyday security and business best practice."

About the PCI Security Standards Council

The PCI Security Standards Council is a global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

# # #